10/519606

#2

PC[illegible]E 03/01067

PRV
PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

Intyg
Certificate

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

(71)	Sökande Applicant (s)	Telefonaktiebolaget L M Ericsson (publ), Stockholm SE
(21)	Patentansökningsnummer Patent application number	0202057-6
(86)	Ingivningsdatum Date of filing	2002-07-02

Stockholm, 2003-06-25

För Patent- och registreringsverket
For the Patent- and Registration Office

Sonia André

Sonia André

Avgift
Fee

1 TITLE OF THE INVENTION

Cookie-receipt Header

2 TECHNICAL FIELD

Mobile Internet Technology

3 PROBLEM

On May 30, 2002 the European Parliament voted in plenary on the amendments tabled by the LIBE Committee on the Council's Common Position on the proposed Directive on data protection in the electronic communications sector.

The result of the vote is to the effect that:

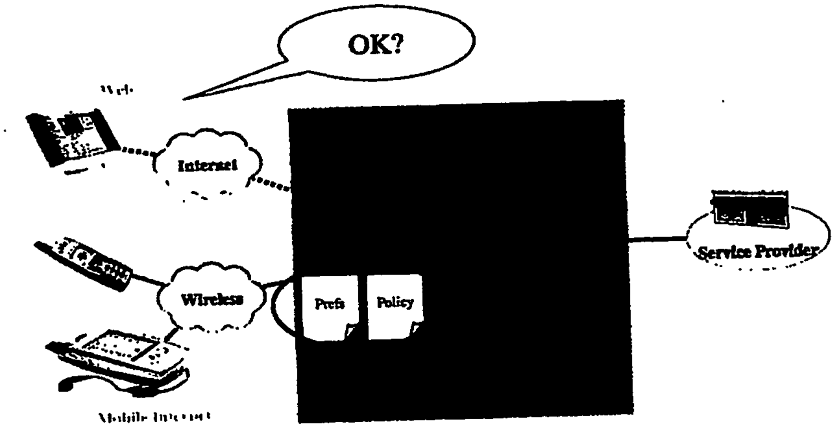
regarding cookies (article 5)

- The use of cookies in EU would only be allowed if the subscriber or user concerned is provided with clear and comprehensive information about the purpose of the cookies (and is offered the right to refuse cookies). This requirement will most likely come into force in EU Member States in October 2003, at the latest.

For implementers of web clients, WAP browsers, or other mobile Internet browsing software, the implication is that a rewrite informing the end-user of events as described above is mandatory. Providers of web services, content providers etc are required to put forth a statement informing the end-user of the fact that cookies will be used in certain locations of the site.

Simply using P3P to subsidize prior information is not enough, since there is today no mechanism to ensure that the policy was indeed read and understood. Thus, we suggest a receipt mechanism, stating that the user-agent handled the cookie policy.

Below is a traditional P3P agreement.



To the left, there is a user-agent that is either placed within or as a plug-in to the browser, or a proxy somewhere within the user's direct or indirect control. A user-agent is simply a piece of software that acts on the user's behalf – and in a P3P scenario, a user-agent is the software that handles the P3P agreement according to the user's preferences.

First, a reference file, containing a sitemap where each resource, or group of resources, at the website is tied to a policy file. This file is generally fetched once per session. Below is an example from the P3P specification of a cookie reference:

```
<META xmlns="http://www.w3.org/2002/01/P3Pv1">
 <POLICY-REFERENCES>
    <POLICY-REF about="/P3P/Policies.xml#first">
       <COOKIE-INCLUDE name="*" value="*"
domain="*" path="*"/>
       <COOKIE-EXCLUDE name="obnoxious-cookie"
value="*" domain=".example.com" path="/"/>
    </POLICY-REF>
    <POLICY-REF about="/P3P/Policies.xml#second">
       <COOKIE-INCLUDE name="obnoxious-cookie"
value="*" domain=".example.com" path="/"/>
    </POLICY-REF>
 </POLICY-REFERENCES>
</META>
```

After this, the policy file for the specific resource can be fetched. It should contain the following (from the specification):

> A cookie policy MUST cover any data (within the scope of P3P) that is stored in that cookie or linked via that cookie. It MUST also reference all purposes associated with data stored in that cookie or enabled by that cookie. In addition, any data/purpose stored or linked via a cookie MUST also be put in the cookie policy. In addition, if that linked data is collected by HTTP, then the policy that covers that GET/POST/whatever request must cover that data collection. For example, when CatalogExample asks customers to fill out a form with their name, billing, and shipping information, the P3P policy that covers the form

submittal will disclose that CatalogExample collects this data and explain how it is used. If CatalogExample sets a cookie so that it can recognize its customers and observe their behavior on its Web site, it would have a separate policy for this cookie. However, if this cookie is also linked to the user's name, billing, and shipping information -- perhaps so CatalogExample can generate custom catalog pages based on where the customer lives -- then that data must also be disclosed in the cookie policy.

In a P3P policy file, one or several statements are defined. These apply to one or several categories of personal identifiable information. Cookies are here referred to as: "#dynamic.cookies" in the DATA tag. Below is an example of a statement referring to cookies in a policy file:

```
<POLICIES
xmlns="http://www.w3.org/2002/01/P3Pv1">
 <POLICY name="forShoppers"

discuri="http://www.catalog.example.com/Privacy/P
rivacyPracticeShopping.html"

opturi="http://catalog.example.com/preferences.ht
ml"
     xml:lang="en">
  <ENTITY>
   <DATA-GROUP>
    <DATA
ref="#business.name">CatalogExample</DATA>
    <DATA ref="#business.contact-
info.postal.street">4000 Lincoln Ave.</DATA>
    <DATA ref="#business.contact-
info.postal.city">Birmingham</DATA>
    <DATA ref="#business.contact-
info.postal.stateprov">MI</DATA>
    <DATA ref="#business.contact-
info.postal.postalcode">48009</DATA>
    <DATA ref="#business.contact-
info.postal.country">USA</DATA>
    <DATA ref="#business.contact-
info.online.email">catalog@example.com</DATA>
    <DATA ref="#business.contact-
info.telecom.telephone.intcode">1</DATA>
    <DATA ref="#business.contact-
info.telecom.telephone.loccode">248</DATA>
    <DATA ref="#business.contact-
info.telecom.telephone.number">3926753</DATA>
   </DATA-GROUP>
  </ENTITY>
  <ACCESS><contact-and-other/></ACCESS>
  <DISPUTES-GROUP>
   <DISPUTES resolution-type="independent"
     service="http://www.PrivacySeal.example.org"
     short-description="PrivacySeal.example.org">
    <IMG
src="http://www.PrivacySeal.example.org/Logo.gif"
alt="PrivacySeal's logo"/>
```

```
    <REMEDIES><correct/></REMEDIES>
   </DISPUTES>
  </DISPUTES-GROUP>
  <STATEMENT>
   <CONSEQUENCE>
     We tailor our site based on your past
visits.
   </CONSEQUENCE>
   <PURPOSE><tailoring/><develop/></PURPOSE>
   <RECIPIENT><ours/></RECIPIENT>
   <RETENTION><stated-purpose/></RETENTION>
   <DATA-GROUP>
    <DATA ref="#dynamic.cookies">
     <CATEGORIES><state/></CATEGORIES>
    </DATA>
    <DATA ref="#dynamic.miscdata">
     <CATEGORIES><preference/></CATEGORIES>
    </DATA>
   </DATA-GROUP>
  </STATEMENT>
 </POLICY>
</POLICIES>
```

For more information about the meaning of this policy, please see "**XML Encoding of Example 3.2**" in the P3P policy specification.

After having processed this information, the user-agent sends a request for the desired page. This is shown as the "GET desired page" in the figure of the traditional P3P agreement. The cookies that have previously been stored are to be sent with this request according to the cookies specification, and the cookie or cookies that are to be stored at the user's side are set with a set-cookie statement in the response header.

4 SOLUTION

We suggest that a receipt be sent with the *GET/POST desired page* request. The two scenarios below handle the cases where the service provider uses this mechanism with P3P-receipt-enabled and non-P3P-receipt-enabled user-agents respectively.

Scenario 1

== Both client and server are P3P-enabled

GET ref file

RESPOND ref file

GET policy

RESPOND policy

GET resource *together with a "I've read and understood your cookies purpose, so don't bother telling me any more" tag*

RESPOND page + cookie (server knows all's well)

==> SERVER BEHAVES IN A VALID WAY

Scenario 2

== User-agent is not P3P-enabled

GET resource *without "read and understood receipt" means either the server does not set a cookie or else it does, but warns the user first*

RESPOND warning + yes/no button

GET resource through yes button

RESPOND resource + cookie

==> SERVER BEHAVES IN A VALID WAY

Note:

P3P also specifies a concept called compact policies, which is a policy included inside the HTTP header of the cookie-setting response, containing information about the cookie to be set.

However, compact policies will not hold as "clear and comprehensive information", since there is no way to know that the cookie was read and understood.

== Corresponding compact policy behavior

GET resource

RESPOND with resource + cookie + policy

==> NOT VALID!!!

After having compared the policy and the user-prefs, a receipt is sent to the service provider, containing information about whether or not the comparison was done using the user's prefs, or whether the user was asked in person. Also, the information tells whether or not it was OK, so that the service provider will know whether or not to bother to send a set-cookie response.

As an additional benefit, the user-agent should remove, and thus not send, cookies set by a server whose policies do not adhere to the user's prefs. We should remember that merely setting the cookie is not a privacy intrusion, but sending it. There are many reasons why a cookie could be set by a site that does not have a policy that corresponds to the user's preferences. One is that the site's policy changed, or that it didn't even exist when the cookie was set, or, correspondingly, that the user's prefs changed.

Receipt	Meaning	Action by user-agent before sending	Action by server before sending set-cookie
P3P: cookie-receipt-user-ok	The user was presented with the policy, and said it was OK to set one.	If there are any cookies stored on the server, they are sent with the receipt.	A set-cookie response header can be sent together with the content, and no additional information should need to be presented to the user.
P3P: cookie-receipt-prefs-ok	The policy was matched with the user's preferences, and it was OK.	If there are any cookies stored on the server, they are sent with the receipt.	A set-cookie response header can be sent together with the content, and no additional information should need to be presented to the user. However, since the user hasn't read the policy in person, info could be written in clear text.
P3P: cookie-receipt-user-nok	The user was asked and said no.	Cookies stored on the server are removed, and if the server sends a set-cookie response (which should be illegal, or at least immoral), it is ignored.	No set-cookie response header should be sent. A note can be presented to the user saying that "since you refused cookies, the service will not function at all/fully..."
P3P: cookie-receipt-prefs-nok	The user's prefs were inconsistent	Cookies stored on the server are removed, and if the server sends a set-cookie response (which should be illegal, or at least immoral), it is ignored.	No set-cookie response header should be sent. A note can be presented to the user saying that "since your prefs are set to refusing cookies, the service will not function at all/fully..."

5 PATENT CLAIM

1. A method for securing that a subscriber is provided with clear and comprehensive information about the purpose of receiving a cookie from a service provider, the method including a traditional P3P agreement with a policy containing information about the cookie to be set and information about the user-prefs,

the method containing the following steps:

- sending a receipt in the "GET desired page" request to the service provider containing information on whether or not a cookie is to be sent to the subscriber and containing information on actions by user-agent and by the service provider.

2. A method for securing that a user has understood the purpose provided by a cookie from a service provider, the method including a traditional P3P agreement with a policy containing information about the cookie to be set and information about the user-prefs,

the method containing the following steps:

- sending a receipt in the "GET desired page" request to the service provider containing information on whether or not a cookie is to be sent to the user and the receipt also containing information on actions to be taken by a user-agent and by the service provider.

6 OTHER COMMENTS

References:

- Cookies: http://wp.netscape.com/newsref/std/cookie_spec.html
- P3P: http://www.w3.org/TR/P3P/